Support for Making Day N Changes to Profiles Attached to a Device

Table 1:

Feature Name	Release Information	Description
Support for Making Day N Changes to Profiles Attached to a Device	NFVIS 4.6.1 Cisco vManage Release 20.6.1	This feature allows you to make changes to Network Design profiles even after they are attached to a device.

Restrictions for Day N Changes in Network Design

- Update from dual WAN to single WAN is not supported.
- Control connections from NFVIS to Cisco SD-WAN Manager can only be established through one path. You can configure either wan-br or wan2-br.
- The SRIOV and OVS interfaces cannot be swapped. This is because the interface MAC addresses are changed.
- Physical ports cannot be removed from the default mapping.
- Only one physical port can be assigned to one OVS-bridge.
- Network mapping swap that results in a MAC address change is not allowed. For instance, changing the VNIC type from virtio to SRIOV is not allowed, as it causes a change in the MAC address.
- Only the CPU and Memory values can be updated in the flavor. We recommend to update the flavor through Cisco SD-WAN Manager.
- We recommend that you first apply the DPDK enabling command alone, to the Day N configuration changes, and after that is successful and the VMs are up and running, then apply the flavor configuration update. This is because, enabling DPDK requires a VM reboot, but when the VM is booting, the VM

flavor cannot be updated. Hence, we recommend that you separate out the DPDK enabling configuration changes from the rest of the configuration changes.

Information About Day N Changes in Network Design

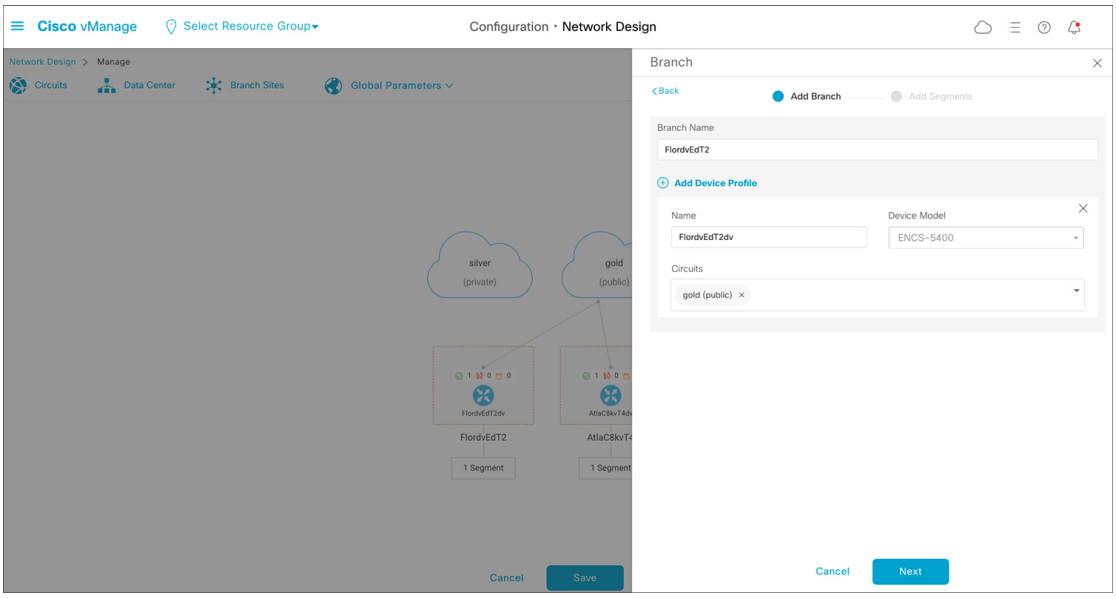
This feature enables you to make changes to the Network Design profiles even after they are attached to one or more devices. You can make changes to the global parameters, edit the services and networks settings, and make changes to the WAN and LAN settings. You can also modify the CLI configuration.

Configure Day N Changes for Network Profiles

Modify Device Name and Branch Name

To change the name of a device that is attached to the network:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Design**.
2. Click **Manage Network Design**.
3. Click **Branch Sites**.
4. Find the device that you want to edit and click the edit symbol.
5. In the **Branch Name** field, enter a name if you want to change the branch name.



6. Click **Next**.
7. If a segment name is not chosen, click the **Segment Name** drop down list and choose a segment name.
8. Click **Add**, and then click **Finish**.

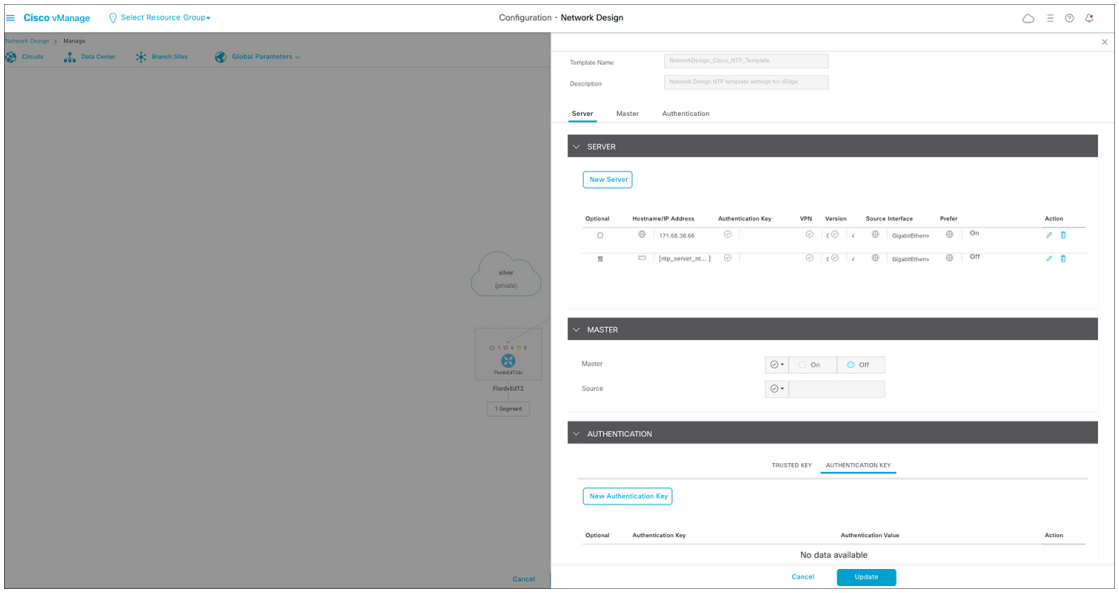
9. Click **Save**. In the dialog box that appears, click **Proceed**.

Modify Global Parameters

Changes in Global Parameters affect all the devices in the network globally. Starting from NFVIS 4.6 release global parameters can be modified even with the devices attached to the network.

To make Day N changes to the global parameters:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Design**.
2. Click **Manage Network Design**.
3. Click **Global Parameters**.
4. From the drop-down list, choose the Cisco IOS XE Catalyst SD-WAN device parameter that you want to modify. You can make Day N changes to these parameters—Cisco NTP, Cisco AAA and Cisco Logging.
5. To add a new server to the profile, click **New Server**, and to add a new authentication key, click **New Authentication Key**. You can modify the existing server and authentication key parameters.
6. You can also modify the **Master** and **Source** parameters.



7. Click **Update**.

Note To configure any NFVIS device changes, use the Cisco IOS XE Catalyst SD-WAN device parameters.

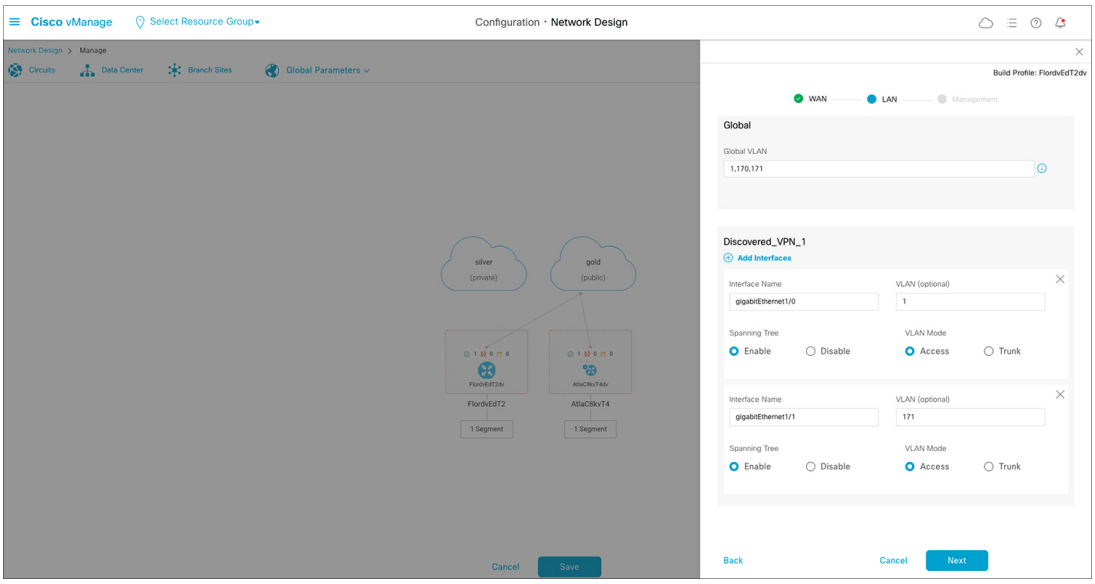
Modify Device Profiles

To make Day N changes to the device profiles:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Design**.
2. Click **Manage Network Design**.
3. Click the device on which you want to make the Day N change.
4. Choose **Edit Profile**.
5. Click the edit symbol to make changes to the parameters.
6. Under **WAN**, set the interface IP to either **DHCP** or **Static**.

Note If you choose the interface IP as static, you need to configure the IP default gateway using the CLI Add-on Feature template.

7. Click **Next**.
8. Under **LAN**, enter the **Global VLAN** value.
9. To add new interfaces, click **Add Interfaces**.
10. To modify settings for the spanning tree, VLAN (VLAN ID), and VLAN mode for the new interface, use the **Spanning Tree**, **VLAN (optional)**, and **VLAN Mode** fields respectively. You can also make these changes for existing interfaces.



11. Click **Next**.
12. Under **Management**, you can set the interface IP to either **DHCP** or **Static** based on your selection in the WAN profile. If you set the interface IP as **DHCP** in the WAN profile, then you need to choose **Static** for the management profile and vice versa.

Note The interface name should not be modified for any of the profiles. The default interface names are:

- For the WAN profile- GE0-0 or GE0-1
- For the LAN profile- gigabitEthernet1/0 through gigabitEthernet1/7
- For the Management profile- mgmt

13. Click **Done**.

Migrating from Insecure to Secure Configuration, Release 26.1.1

Starting from Cisco Catalyst SD-WAN Manager Release 26.1.1, Cisco introduces the **system mode insecure** CLI command. This command is required if your configuration contains insecure features (such as SNMPv1/v2, HTTP, or weak ciphers). To move a device to a fully secure state, you must correct the insecure configurations and then transition the device mode from "Insecure" to "Secure." For more information, see Resilient Infrastructure.

Due to system limitations, this transition cannot be completed in a single configuration push from Cisco SD-WAN Manager. It requires a two-step configuration push process.

Prerequisites

- The device must be running NFVIS and Cisco Catalyst SD-WAN Manager Release 26.1.1.
- You must have an existing Network Design for the branch site.
- A **CLI Add-On Feature Template** must be available to manage the **system mode insecure** command.

Secure the Features (First Configuration Push)

In this step, you update all feature configurations to secure standards to allow the transition.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Design**.
2. Click **Manage Network Design**.
3. Hover your mouse over the image representation of the branch device and choose **Add CLI Configuration**
4. In the CLI Add-On template, add the **system mode insecure** command.
5. Click **Attach Devices** and select the device on the network topology.
6. Choose the specific device from the **Available Devices** list and move it to the **Selected Devices** list using the arrow.
7. Click **Attach**.
8. Click **Config Preview** to verify that both the **system mode insecure** command and all your new secure feature configuration are included.
9. Click **Configure Devices** to push the configuration.

   The configuration updates are pushed to the device. The device features are now secure. However, the device reports the system mode status as `system mode status Insecure`.

Use the **show system mode** command to verify the current system status. To transition the device to a secure status, you must complete the second configuration push to remove the **system mode insecure** command. For more information, see the **Finalize Secure Mode (Second Configuration Push)** section.

Finalize Secure Mode (Second Configuration Push)

To make the device status as Secure, perform the following steps as part of the second configuration push from Cisco SD-WAN Manager:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Design** > **Manage Network Design**.
2. Hover your mouse over the image representation of the branch device and choose **Edit CLI Configuration**
3. Remove the **system mode insecure** command from the template. Alternatively, you may remove the CLI template entirely if it only contains the **system mode insecure** command.
4. Click **Attach Devices** and select the device on the network topology.
5. Choose the specific device from the **Available Devices** list and move it to the **Selected Devices** list using the arrow.
6. Click **Attach**.
7. Click **Config Preview** to that the **system mode insecure** command is no longer present in the configuration.
8. Click **Configure Devices** to push the updated configuration.

   The configuration updates are pushed to the device. This removes the **system mode insecure** command from the device.

   Use the **show system mode** command to verify the current system status. Confirm that the output displays `system mode status secure`. The status will only transition to secure after the second configuration push has successfully removed the **system mode insecure** command.